UNODC
United Nations Office on Drugs and Crime

SHERLOC
SHARING ELECTRONIC RESOURCES AND LAWS ON CRIME

NEWSLETTER ISSUE NO. 13 | DECEMBER 2019

The SHERLOC Team is pleased to share with you Issue No. 13 of our newsletter regarding our recent efforts to facilitate the dissemination of information regarding the implementation of the UN Convention against Transnational Organized Crime and the Protocols thereto, and the international legal framework against terrorism.

Image credit: FBI

In this issue

SPECIAL ISSUE: CYBER ORGANIZED CRIME

Cyber organized crime occurs at the intersection of cyber crime and organized crime. As more and more of our lives takes place in cyberspace, organized crime is also increasingly taking place online. Some organized criminal groups use information and communications technologies to facilitate criminal activity in the offline world. In other organized criminal groups, information and communications technologies are the very basis of how the group is formed. Others still have evolved to include cybercrime among their illicit activities. This special issue of the SHERLOC Newsletter looks at cyber organized crime. It includes a feature of the recent case of *USA v Ramos* which concerned 'Phantom Secure', a company selling custom mobile phones designed to be used by drug traffickers to evade detection. Also included in this issue is information on the SHERLOC team's recent activities in the field of cyber organized crime and our regular 'Meet a Contributor' feature.

FEATURED CASE: *USA V RAMOS* ('PHANTOM SECURE')

Screenshot from Phantom Secure's website

Image credit: Facebook

Mr Vincent Ramos was the founder and CEO of a Canada-based company called Phantom Secure. Phantom Secure sold custom, modified BlackBerry mobile phones. These modified handsets were designed for being impervious to wiretapping, decryption or legal requests to third parties. According to an informant, Phantom Secure's devices were specifically designed, marketed and distributed for use by transnational criminal organizations, specifically those involved in drug trafficking.

In addition to selling the handsets, Phantom Secure also operated an encrypted network that allowed its devices to send and receive encrypted messages. It further offered a subscription to users which allowed Phantom Secure to remotely wipe clients' devices if clients reported that their device had been seized by law enforcement or become compromised, in order to obstruct investigations. Phantom Secure devices and services were provided to clients at a cost of approximately USD 2,000–3,000 per six-month subscription.

Phantom Secure devices were used by senior members of numerous transnational criminal organizations to communicate with their criminal partners and were ultimately used to facilitate the distribution of wholesale quantities of cocaine, heroin and methamphetamines throughout the world, including the United States of America, Australia, Mexico, Canada, Thailand and Europe. US authorities received intelligence that some members of the Sinaloa Cartel in Mexico were users of Phantom Secure devices. Another example of a client of Phantom Secure was Mr Owen Hanson, who used six Phantom Secure devices to coordinate the transportation of more than a tonne of cocaine from Mexico into the United States of America and on to Canada and Australia.

After a news article published on 5 March 2014 stated that law enforcement investigations of a gangland murder were frustrated because the suspects used Phantom Secure devices to coordinate the killing, Mr Ramos wrote that 'this is the best verification on what we have been saying all along – proven and effective for now over nine years. It is the highest level of authority confirming our effectiveness. It can't get better than that.'

US authorities estimated that Phantom Secure generated tens of millions of dollars in revenue through the provision of its services.

Photo advertising Phantom Secure's handsets, posted to Instagram by a Phantom Secure reseller

Image credit: Vice

Phantom Secure laundered the proceeds of its device and services sales through several shell companies. Phantom Secure also used Bitcoin and other cryptocurrencies to launder its earnings.

The organisational structure of Phantom Secure's criminal enterprise included individuals with roles as administrators, distributors and agents. Administrators included Phantom Secure's corporate executives, such as Mr Ramos, and front office staff who had physical control of the Phantom Secure network and its corporate operations. Administrators could initiate new subscriptions, remove accounts and remotely wipe and reset devices. Distributors coordinated agents and resellers of Phantom Secure devices and received commissions for ongoing subscriptions. They also provided technical support and communicated directly with Phantom Secure administrators. Agents physically sourced and engaged with new customers to sell and deliver Phantom Secure devices. They earned a profit on the sale of the handset and provided first-level technical support to their customers.

On 28 February 2018, a warrant for Mr Ramos' arrest was issued by the United States District Court for the Southern District of California. Pursuant to a plea agreement filed 2 October 2018, Mr Ramos pleaded guilty to the charge of a racketeering conspiracy in violation of 18 U.S.C. § 1962(d) and the US agreed to dismiss the charge of conspiracy to distribute narcotics under 21 U.S.C. § 846. On 28 May 2019 the United States District Court for the Southern District of California sentenced Mr Ramos to 9 years' imprisonment.

This feature has been adapted from the original SHERLOC case entry. To find out more about this case, click here to access it on SHERLOC.

RECENT ACTIVITIES

Presentation on cybercrime and the Organized Crime Convention, Abu Dhabi, November 2019

From 17 to 19 November 2019, SHERLOC Consultant Colin Craig attended the *National Conference on Addressing Crime and Violent Extremism: A Collective Responsibility*, held in Abu Dhabi, United Arab Emirates and presented a case study from SHERLOC showing linkages between cybercrime and organized crime and the application of the Organized Crime Convention to the investigation, prosecution and adjudication of cybercrime. The case study examined the interwoven stories of two now-defunct illicit darknet marketplaces, AlphaBay and Hansa Market, showing how US and Dutch investigators, in cooperation with authorities from a number of other countries, successfully tracked down the administrators of the first- and third-largest illicit darknet marketplaces at the time, taking down one of the marketplaces and taking over the other to maximise disruption to the darknet economy.

A case note on the prosecution of the administrator of AlphaBay, Alexandre Cazes, can be found on SHERLOC.

Colin Craig presenting at the National Conference on Addressing Crime and Violent Extremism, Abu Dhabi

Conferences and pre-accession workshops in the Pacific

From 21–22 November 2019, SHERLOC Programme Manager Riikka Puttonen attended the academic *Conference on Linking Organized Crime and Cybercrime* at the University of the South Pacific in Suva, Fiji to present two series of university modules developed by UNODC under the Education for Justice (E4J) initiative on organized crime and cybercrime. The presentation also marked the launch of UNODC's university modules on organized crime for the Pacific. During the conference, Riikka also presented on the links between cybercrime and organized crime, the darknet and the use of cryptocurrencies in organized crime. Riikka also discussed the intersection of cybercrime and organized crime while delivering pre-accession support on the

Riikka Puttonen presenting on cyber organized crime and the Organized Crime Convention in Papua New Guinea

Organized Crime Convention in Solomon Islands and Papua New Guinea in November 2019.

MEET A CONTRIBUTOR

Elise Corsion is a consultant for the Education for Justice (E4J) initiative on organized crime at UNODC. Prior to her consultancy, she was an intern in the Organized Crime Branch, Conference Support Section and contributed to SHERLOC's databases through analysing and uploading to SHERLOC legislation and case law, with a focus on legislation and case law concerning cybercrime and electronic evidence and legal materials in the French language. Prior to interning with UNODC, she also interned at the International Criminal Court in The Hague. Elise holds a master's degree in Public International Law from Leiden University and is currently completing an LLM in Information Technology Law at the University of Edinburgh.

Elise's dedication and attention to detail will be missed by the SHERLOC team!

HAVE YOUR SAY ON THE FUTURE OF SHERLOC

SHERLOC is currently being evaluated with a view to planning the next phase of SHERLOC. As part of this process, we want to hear from you, our users—how you use SHERLOC, what are our strengths and how we can improve. Your feedback can help shape the future of knowledge management of legal resources on organized crime and terrorism.

Please take 5–10 minutes to complete our new user survey, and have your say today.

Click here to access the survey on SHERLOC

Click here to access an additional survey for users of the CNA Directory

Happy Holidays

FROM THE SHERLOC TEAM